

How to Fortinet

Wie eröffne ich einen User mit 2FA über SMS?

Version 1.1





Inhaltsverzeichnis

EINLEITUNG	3
SMS LIZENZ:	3
KONFIGURIEREN EINES USERS MIT SMS-AUTHENTIFIZIERUNG	4
User Konfigurieren:	4
Policy Konfigurieren:	5
RESULTAT:	6



Einleitung

Damit es eine optimale Sicherheit bei der User Authentifizierung gibt, ist die Möglichkeit einen Token anzubinden eine sehr gute Lösung. Dabei gibt der User sein Passwort ein und bekommt noch einen zweiten Faktor zugesendet. Es gibt dabei die Variante, welche dem User eine Textnachricht auf sein Mobile Gerät sendet. Der User muss diesen Zusatz mit eingeben für eine erfolgreiche Authentifizierung.

Auf der FortiGate wird die SMS-Authentifizierung beim User konfiguriert. Wir haben die Möglichkeit den kostenpflichtigen FortiGuard SMS-Dienst von Fortinet zu nutzen.

SMS Lizenz:

Die SMS werden von der FortiGuard ausgelöst. Dieser Dienst ist eine kostenpflichtige Lizenz, welche jeweils 100 SMS enthält.

Der Artikel welcher erworben werden muss:

SMS-ELIC-100 FortiSMS - License for 100 SMS text messages

Der Lizenz Key kann über das folgende Kommando auf die FortiGate eingelesen werden:

```
# execute fortiguard-message add xxxx-xxxx-xxxx-xxxx-xxxx ---> Den Aktivierung  
Code der SMS Lizenz gemäss erhaltenem Dokument einfügen.  
# execute fortiguard-message update
```

Das Guthaben kann folgendermassen über die CLI abgefragt werden:

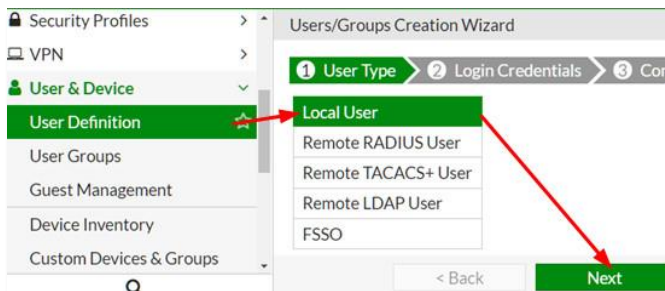
```
# execute fortiguard-message info
```

```
# execute fortiguard-message info  
Controller server status: registered  
Expiry date: 20200102  
SMS max allowed: 4  
SMS used: 4  
Last update: Wed Apr 17 10:31:02 2019  
  
Current message server: 208.91.113.184:443  
Message server status: unknown
```

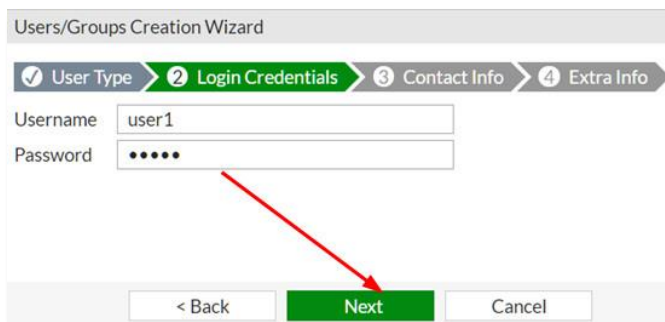
Konfigurieren eines Users mit SMS-Authentifizierung

User Konfigurieren:

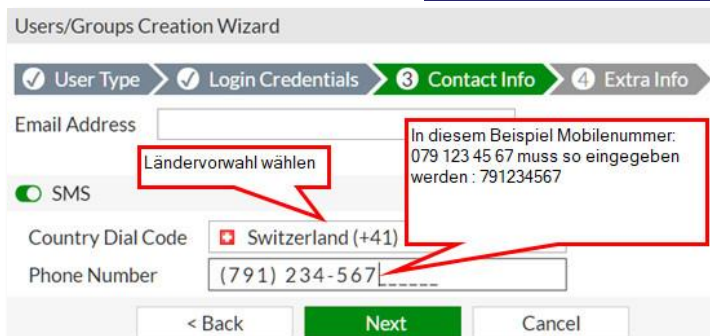
1. User & Device → User Definition -> Create New
2. Local User auswählen, um den User auf der FortiGate zu erfassen



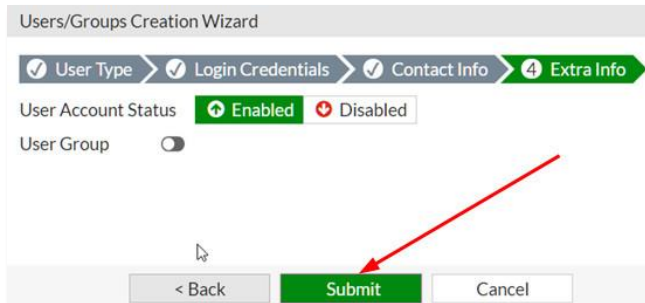
1. Username: Username des Users definieren
2. Password: Passwort für den User definieren



1. optional kann eine Email Adresse angegeben werden
2. SMS-Schalthebel aktivieren
3. Contry Dial Code auf das gewünschte Land setzen
4. Phone Number wird die Mobile Telefonnummer ohne Null voraus angegeben.
Die Mobile Nummer muss im folgenden Format konfiguriert werden:
[Ländercode][Mobilenummer ohne Null voraus]
z.B. 079 123 45 67 wird so hinterlegt : 41791234567
Hinweis: Der Parameter `set two-factor sms` muss über die CLI konfiguriert werden



1. Wenn eine Usergruppe vorhanden ist, kann diese über den Schalter *User Group* ausgewählt werden, so wird der User direkt in diese Gruppe eingefügt
2. *Submit* um den User fertig einzurichten



User über CLI Konfigurieren:

```
config user local
  edit "user1"
    set type Password
    set two-factor sms
    set sms-phone "41791234567"
    set password "password"
  next
end
```

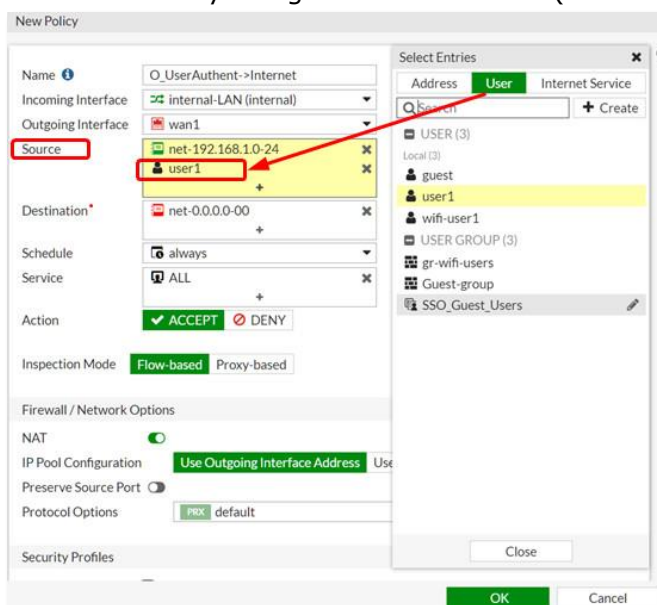


Der `set two-factor sms` Parameter ist wichtig, damit dem User mitgeteilt wird, dass die SMS Two Faktor Authentifizierung aktiviert wird. Leider ist diese Option im WebGui beim User erst ersichtlich, wenn sie auf der CLI einmal konfiguriert wurde.

Policy Konfigurieren:

Jetzt muss der User bei der entsprechenden Regel in die Source eingeführt werden.

1. Policy *Source* auf *User* gehen und den User oder die Gruppe auswählen
2. Die Policy wie gewohnt einrichten (Destination Services Nat usw....)



Bei der Policy muss der User in der Source angegeben werden, damit die Authentifizierung zieht. In dieser Regel sind ANY Services konfiguriert. Für einen produktiven sicheren Betrieb empfiehlt sich nur die Services freizuschalten, welche auch benötigt werden. Weiter empfiehlt es sich entsprechende UTM Features zu aktivieren, um sich optimal abzusichern

Policy über die CLI konfigurieren:

```
config firewall policy
  edit <POLICY-ID>
    set name "O_UserAuthent->Internet"
    set srcintf "internal"
    set dstintf "wan1"
    set srcaddr "net-192.168.1.0-24"
    set dstaddr "net-0.0.0.0-00"
    set action accept
    set schedule "always"
    set service "ALL"
    set logtraffic all
    set users "user1"
    set nat enable
  next
end
```

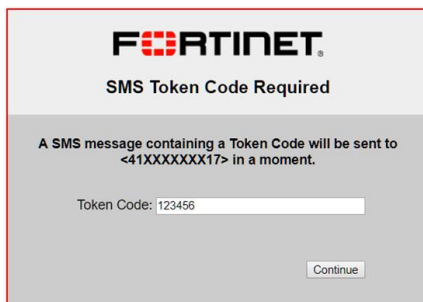
Resultat:

Wenn wir jetzt eine Anfrage über den Webbrowser in das Internet vornehmen, wird ein Logging Fenster im Browser erscheinen



The dialog box has a grey header with the Fortinet logo and the text 'Authentication Required'. Below this, it says 'Please enter your username and password to continue.' There are two input fields: 'Username: user1' and 'Password: *****'. A 'Continue' button is at the bottom right.

Nachdem sich der user1 mit seinem Passwort authentifiziert hat, kommt noch die SMS-Abfrage. Der User hat jetzt 60 Sekunden Zeit den SMS-Code einzutippen. Nach dieser Zeit ist der ausgelieferte Code ungültig



The dialog box has a grey header with the Fortinet logo and the text 'SMS Token Code Required'. Below this, it says 'A SMS message containing a Token Code will be sent to <41XXXXXXXX17> in a moment.' There is an input field for 'Token Code: 123456'. A 'Continue' button is at the bottom right.